UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEIZURE AND SEARCH OF: **PNY PERFORMANCE 4GB SD CARD**	**CASE NO.** 1:21-mj-259 TMD

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeffrey A. Yesensky, being duly sworn, do hereby depose and state:

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and I have been so employed since November 2005. I am currently assigned to a multi-agency child exploitation task force known as the Baltimore Maryland Child Exploitation Task Force. Since September 2009, my responsibilities in the FBI have primarily involved the enforcement of federal criminal statutes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2251, *et seq*. As part of my training, I have attended numerous training classes regarding the Internet, on-line child pornography, Internet child enticement, child sex trafficking, and child sex tourism, and have consulted with my colleagues who have many years of experience investigating child pornography and child exploitation cases. I have also been the affiant on numerous prior search and arrest warrants.[1]

[1] On May 8, 2014, in *United States v. Walter L. Williams* (C.D. Cal. 13-302-PSG), Special Agent Yesensky testified in a hearing regarding a border seizure and later warranted search of two laptop computers. In the search warrant affidavit, Special Agent Yesensky accounted for a delay in seeking the warrant due to an "oversight on my part due largely to demands of two forensic reviews that I was conducting concurrently of two computers in separate investigations, which each involved the review of hundreds of thousands of images."

While testifying before the district court, Special Agent Yesensky was asked to explain the "context" for the referenced portion of his search-warrant affidavit. Special Agent Yesensky testified that, during the seizure, he was also giving priority to other matters, such as leading a task force responsible for assisting 18-20 victims of child prostitution.

In a May 9, 2014 written opinion, the district court judge wrote that he "[did] not find this additional statement to be credible" and that the new statement "contradicts" his prior testimony. The judge wrote: "How could Agent Yesensky have 'overlooked' his duty to procure a warrant while simultaneously 'prioritizing' other matters?" In response to the district court's opinion, the United States Attorney's Office for the Central District of California and the Child

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute arrest and search warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for: a PNY PERFORMANCE 4GB SD CARD WITH SERIAL NUMBER WZ40614 (the "TARGET DEVICE") , which is more specifically described in Attachment A to this Application, for contraband and evidence, fruits, and instrumentalities of Title 18 U.S.C. § 2252A(a)(2) (receipt and distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) (hereinafter the "SUBJECT OFFENSES") which items are more specifically described in Attachment B to this Affidavit.

4. The statements in this affidavit are based in part on information provided by the Frederick County Sheriff's Office and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe

---

Exploitation and Obscenity Section of the Criminal Division of the United States Department of Justice filed a Motion for Reconsideration urging the judge, for a variety of reasons, to revisit the district court's credibility finding as unsupported under the circumstances. The district court denied the Motion for Reconsideration on June 20, 2014.

On October 1, 2014, the Assistant Director in Charge (ADIC) of the FBI-Los Angeles Field Office (LAFO) memorialized LAFO's finding that the district court opinion did not warrant referral to the FBI's Office of Professional Responsibility for a lack of candor or any other investigative deficiency. In the executive summary of the non-referral statement, the ADIC wrote that, "The facts and circumstances of this case clearly indicate that SA Yesensky was not making any misrepresentation to the court. All prosecutors with intimate knowledge of the case disagree with the lack of credibility finding and supported the motion to reconsider that decision."

The district court's two Opinions, the Motion for Reconsideration (including the lead prosecutor's sworn Affidavit), the FBI's non-referral letter and executive summary, and the suppression hearing transcript are available to this Court upon request.

Since the issuance of the district court's opinion, Special Agent Yesensky has obtained over 35 federal search warrants for electronic accounts, digital devices, and residences in multiple district courts.

are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of the TARGET OFFENSES are located on the TARGET DEVICE.

DEFINITIONS

5. The following definitions apply to this affidavit and attachments:

a. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

b. "Computer", as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

c. "Computer hardware", as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, laptops, tablets, eReaders, Notes, iPads, and iPods; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, SD cards, thumb drives, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including, but not limited to keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "Computer software", as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the Internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers" (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

j. "An Internet Protocol address" (IP address) is a unique numeric address used by Internet-enabled electronic storage devices to access the Internet. Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

k. "Child Pornography," as used herein, is defined pursuant to Title 18, United States Code, Section 2256(8), as "…any visual depiction, including any photograph, film, video,

picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct."

l. The term "minor," as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1), as "any person under the age of eighteen years."

m. The term "sexually explicit conduct," as used herein, is defined pursuant to Title 18, United States Code, Section 2256(2) as "actual or simulated—(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person."

n. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See Title 18, United States Code, Section 2256(5).

o. The terms "documents" and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BITTORRENT PEER TO PEER NETWORKS

6. Peer to Peer (P2P) file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software from a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. BitTorrent, one type of P2P software, sets up its searches by keywords typically on torrent websites. The results of a keyword search are displayed to the user.

The website does not contain the files being shared, only the file referred to as a torrent. The user then selects a torrent file(s) from the results for download. This torrent file contains instructions on how a user can download the file(s) referenced in the torrent. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the actual files (not the torrent file but the actual files referenced in the torrent file using any BitTorrent client.)

7. For example, a person interested in obtaining child pornographic images would open the BitTorrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a torrent file from the results displayed the file(s) he/she wants to download. Once the torrent file is downloaded, it is used by a BitTorrent program, which the user had previously installed. The torrent file is the set of instructions the program needs to find the files referenced in the torrent file. The file(s) is downloaded directly from the computer or computers sharing the file. The downloaded file(s) is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.

8. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file.

9. The computer running the file sharing application, in this case a BitTorrent application has an IP address assigned to it while it is on the Internet. BitTorrent users are able to see the IP address of any computer system sharing files to them or receiving files from them.

Investigators log the IP addresses, which have sent those files or information regarding files being shared. Investigators can then search public records (ARIN) that are available on the Internet to determine the Internet service provider who has assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the Internet service provider.

10. Millions of computer users throughout the world use P2P file sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

11. The BitTorrent network is a very popular and publically available P2P file-sharing network. Most computers that are part of this network are referred to as "peers" or "clients". A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

12. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publically available and typically free P2P client software programs that can be downloaded from the Internet.

13. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading[2]. Typically, as users download files or pieces of files from other peers/clients on the

[2] As an example, during the downloading and installation of the publically available uTorrent client program, the license agreement for the software states the following: "Automatic Uploading. uTorrent accelerates downloads by enabling your

BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding".

14. Files or sets of files are shared on the BitTorrent network via the use of torrents. A torrent is typically a small file that describes the file(s) to be shared. It is important to note that torrent files do not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish a download. This information includes things such as the name(s) of the file(s) being referenced in the torrent and the "info hash" of the torrent. The "info hash" is a SHA-1[3] hash value of the set of data describing the file(s) referenced in the torrent. This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each torrent uniquely identifies the torrent file on the BitTorrent network. The torrent file may also contain information on how to locate file(s) referenced in the torrent by identifying "Trackers". "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s)

computer to grab pieces of files from other uTorrent or BitTorrent users simultaneously. Your use of the uTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded.

3 The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

referenced in the torrent file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the torrent. "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular torrent file. There are many publically available servers on the Internet that provide BitTorrent tracker services.

15. In order to locate torrent files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include isohhunt.com and the piratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate torrent files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by torrent files, only the torrent files themselves. Once a torrent file is located on the website that meets a user's keyword search criteria, the user will download the torrent file to their computer. The BitTorrent network client program on the user's computer will then process that torrent file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the torrent file. It is again important to note that the actual file(s) referenced in the torrent are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 info hash value comparison), or parts of the same file(s), referenced in the torrent, to include the remote peers/clients Internet Protocol (IP) addresses.

16. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a torrent of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the torrent file. Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the torrent file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the torrent file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

17. Law Enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. Searching the network for these known torrents can quickly identify targets in their jurisdiction. Law Enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA-1 hash values of torrents. These

torrents being searched for are those that have been previously identified by law enforcement as being associated with such files. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network. I knows through my training, knowledge, and experience that it is not always possible to complete a download from a suspect device. Several factors can inhibit the download from a suspect device including network issues and software settings. This information can be documented by investigators and compared to those info hash SHA-1 hash values the investigator has obtained in the past and believes to be child pornography. Therefore, without even downloading the file, the investigator can compare the info hash SHA-1 value and determine with mathematical certainty that a file(s) seen on the network is an identical copy of a child pornography file(s) they had seen before.

18. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer. Law enforcement has the ability to log this information.

19. The investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the sexual exploitation of actual child victims.

INVESTIGATIVE FACTS

20. In July 2020, I received information from the Frederick County Sheriff's Office ("FCSO") regarding the FCSO investigation of JEFFREY JOHN WHITE ("WHITE"), who was a Registered Sex Offender in Maryland and being investigated by the FCSO for the distribution, receipt, and possession of child pornography via BitTorrent. As a result of the FCSO investigation, WHITE was arrested by the FCSO on July 6, 2020, and charged in the State of Maryland with 10 counts of child pornography distribution in violation of Maryland Code CR Section 11.207(a)(4). The FCSO requested assistance with its investigation from the FBI and eventually provided the FBI with FCSO case files from the investigation of WHITE. During my review of the FCSO case files, I learned the following, among other things:

21. On April 14, 2020, an undercover computer ("UC") in the FCSO office, located in Frederick, Maryland, began conducting an online investigation on the BitTorrent network for offenders sharing child pornography. Investigative focus was directed to IP address 73.200.141.134 because it was associated with several torrents identified as being of investigative interest for child pornography investigations.

22. Using a computer running investigative BitTorrent software, between approximately April 14, 2020, and April 24, 2020, the UC directly connected to the device at IP

address 73.200.141.134 (herein after the "suspect device") and performed several downloads, or partial downloads, of files containing child pornography. The suspect device reported it was using BitTorrent software version 4.2.3. Some of these downloads by the UC are summarized below, in part:

23. On April 14, 2020, at 1541 hours, the UC made a successful connection to the suspect device at IP address 73.200.141.134, port 55962. During this connection, the suspect device reported it was in possession of 20 pieces contained in the torrent with info hash: ad5a4097da538b4cbc9a0dd377bb039be42b1830, which contained 18 files. The connection was terminated on April 15, 2020, at 0117 hours. The FCSO was able to verify the info hash ad5a4097da538b4cbc9a0dd377bb039be42b1830 contained child pornography. Not every file in the info hash successfully downloaded from the suspect device. Of the files that did download, several were confirmed to contain child pornography. One example is summarized below:

a. Video file titled "Youngvideomodels - I04n - Irina 12yo (nude).avi – video" that depicts a naked pubescent female, approximately 12-years old, sitting on a chair with her legs open and her bare vagina exposed to the camera. During this video, the girl uses her hands to spread apart her vagina.

24. On April 15, 2020, at 0117 hours, another connection was made by the UC to the suspect device at IP address 73.200.141.134, port 55962. The suspect device reported it possessed torrent with info hash: a8d8436a9b5f04ea27eaa277584f44095a33e6f3, which contained 18 files and the suspect device reported having 111 pieces. The download was completed at 0802 hours on April 15, 2020. The FCSO was able to confirm that the files contained child pornography. This torrent is known to be part of a series that contain files of investigative interest for child exploitation material. One file that was downloaded in summarized below:

a. Video with file name "lsm02-06-02.mpg" that depicted two pubescent females, between 14-16 years of age, dancing naked. During this video, on several occasions, the camera is focused on the girls' vaginas.

25. On April 23, 2020, the UC made several connections with the suspect device reported to be at IP address 73.200.141.134, port 61315. Some of these connections are summarized below, in part:

a. At 0428 hours, the suspect device reported to be in possession of torrent info hash: f858306a74644f435edc7d953d7df8b647cc68a7, of which it acknowledged having 841 pieces. This info hash is known for investigative interest of child pornography. The FCSO was able to confirm it contained child pornography;

b. At 0448 hours, the suspect device reported to be in possession of torrent info hash: 3832a0f683b39a0e8302d843413f766d258271b3, of which it acknowledged having 1255 pieces. The download was not complete and the connection was terminated at 0517 hours on April 23, 2020. The FCSO knew this torrent is one of investigative interest with regards to child pornography;

c. At 0450 hours, the suspect device reported to be in possession of torrent with info hash: 3832a0f683b39a0e8302d843413f766d258271b3, of which it acknowledged having 1255 pieces. The download was not complete and the connection was terminated at 0517 hours on April 23, 2020. The FCSO knew this torrent is one of investigative interest with regards to child pornography.

26. On April 24, 2020, the UC made two connections to the suspect device o at IP address 73.200.141.134, port 57932, which are summarized below, in part:

a. At 00:53:20 hours, the suspect device reported to have torrent info hash: f858306a74644f435edc7d953d7df8b647cc68a7, of which it acknowledged having 842 pieces. This download was stopped at 0457 hours. The download was not completed; however; the info hash is known to be of investigative interest for child pornography;

b. At 00:53:37 hours, the suspect device reported to have torrent info hash: f858306a74644f435edc7d953d7df8b647cc68a7, of which it acknowledged having 842 pieces. This download was stopped at approximately 0457 hours and was not completed; however the info hash is known to be of investigative interest for child pornography.

27. On June 14, 2020, the FCSO obtained records from Comcast Cable Communications for IP address: 73.200.141.134 which listed the subscriber of this IP Address since February 20, 2018, to be "Jeffrey White" and the Service/Billing Address to be "9 S 2nd St Unit C, Woodsboro, MD 21798."

28. The FCSO identified WHITE, who resided at 9 South 2nd St Unit C, Woodsboro, MD 21798, to be a Registered Sex Offender who was currently on probation for a child pornography conviction from approximately 2014. The FCSO noted that WHITE's previous case revealed he was a collector of child pornography, and in that case, WHITE was found to have over 4,000 images and 14 videos of child pornography, as well as files of child erotica on USB drives, in addition to over 5,000 images and 56 videos found on his laptop.

29. On June 25, 2020, the FCSO obtained a search and seizure warrant for WHITE's residence located at 9 South 2nd St., Unit C, Woodsboro, MD 21798, from the Honorable Judge Julia Martz Fisher. On July 6, 2020, this warrant was executed by the FCSO, with assistance from the FBI, and the FCSO seized the following item that belonged to WHITE from his residence: One HP Probook 650 GT laptop with S/N: 5CG5181YKG (hereinafter "HP Probook Laptop").

30. WHITE was interviewed by the FCSO and myself during the execution of the above search warrant and provided voluntary statements to law enforcement officers after waiving his Miranda Rights. During this interview, WHITE identified the HP Probook Laptop as belonging to him and being used solely by him, and WHITE repeatedly told the interviewing agents he did not know the password to the HP Probook Laptop, despite changing the password to it some time prior.

31. The HP Probook Laptop was found to be encrypted and, therefore, could not be accessed initially by the FCSO. On July 22, 2020, the FCSO requested assistance from the FBI with the decryption of the HP Probook Laptop.

32. On or about October 9, 2020, the FBI's successfully decrypted the hard drive of the HP Probook Laptop and created a decrypted forensic image of its contents. This decrypted image

was thereafter returned to the FCSO on October 13, 2020, for review by the FCSO. During this review, the FCSO's found the HP Probook Laptop to contain approximately 7,000 unique image files and approximately over 240 unique video files considered to be suspected child pornography, which included the following:

a. Video file, with file name "3A94DCFC8F2CF2BF864372292F032321.mp4" that depicts naked prepubescent minor female, aged approximately 8- to 11-years old, in a seated position with her legs spread apart such that her bare vagina is exposed to the camera. The hand of an apparent adult male is observed in this video using two fingers to spread the vagina apart to take a close-up of her vagina;

b. Video file, with file name "17BCD158E8BB29C6593EE12447728CA1.mkv" that depicts a prepubescent minor, aged approximately 9- to 11-years old, wearing no bottoms and laying on her bed on her back with a cat. The minor is observed spreading her legs, exposing her bare vagina to the camera, and rubbing her vagina with her hands. The minor is also depicted on her knees, on the bed, exposing her bare vagina and anus to the camera while she uses her finger to rub her anus and vagina.

33. On December 7, 2020, following the above forensic assistance provided by the FBI, the FBI returned HP Probook Laptop to the FCSO, whereupon the FCSO observed the presence of the TARGET DEVICE inside the HP Probook Laptop.

34. The TARGET DEVICE has remained in the secured custody of the FCSO and or FBI since its seizure from WHITE's residence on July 6, 2020, by the FCSO. While in the secure custody of the FCSO and the FBI, the TARGET DEVICE was not searched. The FBI did not conduct a search of the TARGET DEVICE at the time of the above decryption and forensic processing of the HP Probook Laptop; only the hard drive of this laptop was forensically processed.

35. The TARGET DEVICE is currently in the secure custody of the FBI at the FBI Office in Linthicum, Maryland.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS, AND/OR DISTRIBUTE CHILD PORNOGRAPHY

36. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have an interest in child pornography and who possess and/or distribute child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or in other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, and child erotica, etc. for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers

of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

37. Based on the following, I believe WHITE displays characteristics common to individuals who possess and/or distribute child pornography: As described above, on multiple occasions, between approximately 2013 and 2020, WHITE was found to have possessed and/or shared numerous sexually explicit images and videos depicting minors.

CONCLUSION

38. Based on the foregoing, I respectfully submit there is probable cause to believe the SUBJECT OFFENSES have been committed, and there is probable cause to believe evidence of these crimes can be found on the TARGET DEVICE.

39. Because the search of the TARGET DEVICE will be of an object already in the custody and control of the FBI, and will not require any intrusion upon physical premises, I respectfully submit that good and reasonable cause exists to permit the execution of this warrant at any time, day or night.

[SPACE INTENTIONALLY LEFT BLANK]

Special Agent Jeffrey A. Yesensky
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) on this 1 day of February, 2021.

Honorable Thomas M. DiGirolamo
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE DEVICE TO BE SEARCHED

The device to be searched is a PNY PERFORMANCE 4GB SD CARD WITH SERIAL NUMBER WZ40614 ("TARGET DEVICE") that is in the custody of the FBI and located at an FBI facility in Linthicum, Maryland.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252A(a)(2) (receipt and distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography):

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of 9 SOUTH SECOND STREET, UNIT C, WOODSBORO, MD 21798, including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.

6. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

7. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

8. If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

9. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

10. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.